United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Defense, Committee on Appropriations, House of Representatives

June 1992

# ATTACK WARNING



# Lack of System Architecture Contributes to Major Development Problems



GAO/IMTEC-92-52

GAO

**United States**
**General Accounting Office**
**Washington, D.C. 20548**

**Information Management and**
**Technology Division**

B-248608

June 11, 1992

The Honorable John P. Murtha
Chairman, Subcommittee on Defense
Committee on Appropriations
House of Representatives

Dear Mr. Chairman:

For a decade the Air Force has been modernizing computer subsystems in Cheyenne Mountain, the command center for the North American Aerospace Defense Command's (NORAD) Integrated Tactical Warning and Attack Assessment (ITW/AA) system. This effort—designated the Cheyenne Mountain Upgrade (CMU) program—is intended to modernize systems that provide critical strategic surveillance and attack warning and assessment information to U.S. and Canadian leaders. Because of your continuing interest in this program, you requested that we review Air Force activities to complete this effort—specifically, the impact of not using an overall system architecture to guide CMU design and development. Appendix I provides a detailed description of our objectives, scope, and methodology.

## Results in Brief

The Air Force continues to develop the CMU program as five individual subsystems without an overall system architecture, increasing the risk that CMU will not operate as an integrated unit. The absence of an overall CMU architecture that describes system and subsystem relationships and requirements and establishes standards to guide development has contributed to a CMU system that cannot meet original system requirements and cannot easily evolve to meet the needs of new missions. Until the Air Force performs the analyses needed to define an overall CMU system architecture and determines what capabilities are required for each subsystem to meet system requirements, it will continue to face serious development and integration problems and will have a system that cannot easily accommodate mission changes.

The Air Force's development approach is driven by cost and schedule. The Air Force has told the Congress it can complete the system for $1.58 billion by 1995. In reality, it is deferring some CMU requirements, completing only those that its development budget and schedule will allow. Consequently, the Air Force is developing a system with less capability than originally planned, since the deferred requirements are to be completed only after delivery of the system.

## Background

NORAD is responsible for warning U.S. and Canadian leaders when North America is under air, missile, or space attack. This mission is supported by the automated ITW/AA system designed to identify and track enemy objects. ITW/AA is a system-of-systems consisting of ballistic missile, space, and atmospheric warning systems; intelligence centers; associated communications links; and command and control centers. Cheyenne Mountain Air Force Base houses data processing and communications equipment supporting the ITW/AA system. In 1981 the Air Force began a modernization effort consisting of five separate acquisitions to replace aging and obsolete computer subsystems at Cheyenne Mountain.[1]

The five acquisitions were initially planned to be completed in 1987 at a cost of $968 million. In 1989 the Air Force responded to congressional concern over subsystem integration problems by combining the five into one program, the Cheyenne Mountain Upgrade (CMU), and committing to completion by December 1995 at a cost of $1.58 billion. However, as we reported in 1991, this cost estimate does not include funding for all requirements; the costs for completing a fully functional, mission-ready system will surpass $1.9 billion.[2]

## Lack of Overall System Architecture Contributes to Increased Costs and Subsystem Problems

The Air Force did not use a system architecture, or overall plan, to guide the design, development, and integration of the CMU subsystems. Instead, these subsystems were designed and continue to be developed as five separate subsystems, even though they are required to work together as an integrated unit. According to the Air Force's CMU program element monitor, the Air Force did not develop a CMU system architecture when the five programs were consolidated in 1989 because any resulting changes to the subsystems would have had a significant cost and schedule impact. The lack of a CMU architecture to guide system and subsystem development has contributed to a costly, problem-laden system that cannot easily adapt to changing mission needs.

[1]The five subsystems are the (1) Communications System Segment Replacement (CSSR); (2) Space Defense Operations Center 4 (SPADOC 4); (3) Command Center Processing and Display System Replacement (CCPDS-R); (4) Survivable Communications Integration System (SCIS); and (5) Granite Sentry. The backup system, added in 1989, is the Offutt Processing and Correlation Center (OPCC) at Offutt Air Force Base in Nebraska; it will provide missile warning and air defense information should the system at Cheyenne Mountain fail. Appendix II contains additional information on these subsystems.

[2]Attack Warning: Costs to Modernize NORAD's Computer System Significantly Understated (GAO/IMTEC-91-23, Apr. 10, 1991).

## The Importance of a System Architecture

System architectures provide a basis for planning and guiding development to ensure interoperability and compatibility between and among subsystems. Through detailed analysis, they define the most effective approach to meet current as well as potential future mission needs before beginning the acquisition process. They also describe and influence the hardware, software, communications, data base management, and security characteristics for a system.

A system architecture is derived from a strategic information systems planning process—a structured approach to systematically identifying and defining an organization's near- and long-term information and processing needs. The planning process includes clearly defining the organization's current and future missions and identifying the system's functional and operational requirements. Such requirements specify the level of performance needed to accomplish the missions and provide the information that will govern overall system design and development and hardware and software choices. Architectures emphasize system and subsystem interdependence. System architectures also recognize interplay among components, that is, they define the system's required operational effectiveness, maintainability, and flexibility to adapt to changing missions; the degree to which the system must be expandable or upgradable to meet future needs; and its ability to incorporate technological improvements.



In contrast, CMU program managers are developing their respective subsystems to individual design specifications. These specifications, however, provide detail only on the individual subsystems—not on the system as a whole—and thus, even in aggregate, are not acceptable substitutes for an overall system architecture. While the Air Force has developed a CMU system operational requirements document, it does not contain the information necessary to adequately guide the design and development of the integrated CMU program. No CMU architecture exists that defines how the five subsystems are to work together and how standards[3] are to be used to ensure that the five subsystems under development will be compatible, interoperable, and adaptable to change. Consequently, hardware choices were made before processing needs were adequately analyzed and understood. These premature choices resulted in the need to replace hardware and modify software to achieve performance

[3]Standards are rules, laws, customs, specifications, or practices that are considered by authorities or by general consensus which when applied will provide a basis for comparison or fulfilling specific requirements.

requirements. Further, software is being developed that cannot easily adapt to mission changes.

## CMU Hardware Decisions Have Necessitated Expensive Modifications

The Air Force acquired CMU subsystem hardware without having thoroughly defined either subsystem- or system-level requirements. Nor did the Air Force consider the potential impact of future missions. Had the Air Force used a structured approach to develop a CMU system architecture, it would have performed a detailed analysis to identify the types and amount of information that must be processed and shared among subsystems. This analysis would have formed the basis for selecting subsystem hardware.

However, the Air Force made hardware selections in the absence of thorough system or subsystem requirements analyses. Three examples illustrate that premature hardware selection has been costly and has contributed to performance problems. First, the Air Force spent $24 million to upgrade SPADOC 4 hardware from the IBM model 3083 to the model 3090 because the model 3083 did not have sufficient processing capacity. The Air Force had not adequately analyzed the requirements for real-time data processing combined with stringent security requirements prior to hardware selection.

Second, the Air Force did not adequately define SCIS workload requirements and allowed the developer to select hardware based on the developer's interpretation of the work load. When the Air Force later defined its requirements, which increased the work load on the system, the developer's hardware proved inadequate. As a result, SCIS program hardware had to upgraded at an estimated cost of over $28 million.

Finally, the Air Force's use of flow controls for CSSR illustrates how software "work arounds" and hardware upgrades have been used to compensate for poor hardware choices. The total ITW/AA message load—including messages coming into, going out of, and being routed between and among command centers within Cheyenne Mountain—was not adequately defined when the five upgrade programs started. This oversight resulted in having to upgrade the CCPDS-R hardware and design and develop software to screen and prioritize messages being processed by CSSR—a technique known as flow control. Because CSSR still could not process all the messages required, some processing was shifted to CCPDS-R, which increased its message processing requirements beyond the capability of the CCPDS-R hardware. As a result, the Air Force spent

between $5 million and $6 million upgrading the CCPDS-R hardware from Digital Equipment Corporation VAX 6420 to VAX 6430 to meet the higher message processing requirement. Had the Air Force adequately analyzed the workload processing requirements for the CMU subsystems, these expensive, time-consuming modifications might have been avoided.

## MU Software Cannot Be asily Modified

To meet subsystem requirements, developers tailored software to optimize the performance of the chosen hardware. Because the software reflects specific hardware characteristics, it cannot be easily modified to run on other hardware, i.e., newer, more powerful platforms or other vendors' equipment. Thus, it is difficult for the Air Force to incorporate new technology as it is offered in the marketplace.

The Air Force should not have allowed this to happen. It should have provided contractors with a consistent standard framework for software development to ensure that software would work on different manufacturers' hardware. Instead, the Air Force provided no requirement or specific guidance to CMU developers to achieve this desired software portability, as evidenced by the CCPDS-R specification section describing portability requirements, which simply read "not applicable." As a result, CMU software is not very portable. As the hardware used on CMU subsystems is replaced due to changes in processing requirements or mission, the Air Force will be faced with costly and time-consuming software reengineering. This is currently happening on the SCIS program where the Air Force has changed from a hardware platform that used Tolerant Corporation hardware to one that now uses Digital Equipment Corporation hardware. Of the 341,000 lines of software code needed for the Digital Equipment Corporation hardware, only 155,000 lines (45 percent) originally written for the Tolerant hardware are portable to the new Digital hardware.

Further, because no systemwide security architecture exists, each contractor selected hardware and software based on its interpretation of what is needed to provide for a secure system. Accordingly, the subsystem contractors are implementing security controls somewhat differently. For example, the SPADOC 4 contractor decided to embed required security functions into the application software. This approach differed from the Granite Sentry contractor, who provided security through the commercially available operating system. Such non-uniform and unstru· tured approaches to security not only increase the complexity of makin, changes, but also increase the risk that, once the subsystems are

connected, the system will not be able to provide the needed level of protection.

## Air Force Is Not Effectively Planning for CMU to Interface With Future Systems

The Air Force realizes that it needs a system that can be modified to accommodate changing threats and one that must effectively interface with new systems to address those threats. However, the CMU program is essentially being built to interface with the operational systems that will exist when CMU becomes operational but will not be capable of meeting the requirements of future missions. Further, and equally disturbing, is that resources are not currently planned or programmed to modify CMU to interface with a multitude of future systems that are currently being considered. These include antisatellite defense, ballistic missile defense, Follow-on Early Warning System, Relocatable Over-the-Horizon Radar, and Mobile Command Centers, to mention a few.

These additional requirements will have a profound impact on the CMU subsystems. SPADOC 4, for example, will have to be significantly changed to meet the increased processing work load that will be required to support the antisatellite defense mission requirements. Similarly, CSSR does not have the processing capacity to support other missions, such as ballistic missile defense. The Air Force's March 1992 CMU System Operational Requirements Document discusses this deficiency in CMU capability. The document warns the Air Force that unless the CMU program is changed to accommodate future missions, it will not receive the benefit of improved data, nor will it be able to operate in concert with the new systems. Further, the document recognizes a significant impact to the new systems under development—it cautions that they will not benefit from the data that CMU could provide and that the developers of those systems may have to spend a significant amount to duplicate capabilities that CMU could provide.

## CMU Will Not Provide Originally Promised Capabilities Within Congressional Cost Ceiling

The Air Force continues to tell the Congress that CMU will be completed by 1995 at a cost of $1.58 billion. This represents a schedule delay of 8 years and a cost increase of at least $600 million. The Air Force has changed the meaning of "completed" by meeting only those requirements its budget and schedule will allow and is deferring the rest until after 1995. In April 1991 we reported that the costs for the program were seriously

understated and that some system requirements were being deferred to keep the program within its near-term cost and schedule goals.[4] We pointed out that funding for items such as software changes, acquisition of selected high-speed communication circuits, hardware maintenance, and engineering support were not included in the Air Force's cost estimate.

The Air Force plans to develop deferred capabilities at a later date through a preplanned product improvement program to be instituted after the system is delivered in 1995. Because the $1.5 billion limit will have been reached, deferred capabilities would be completed with funds used to operate and maintain CMU, according to the program element monitor.

## Conclusions

CMU is an example of how not to build a system—it exemplifies the pitfalls of independently building subsystems that must work together in an integrated environment without an overall system architecture to guide design and development. The Air Force is acquiring subsystems without a clear understanding of how they are to operate together, that have had numerous hardware and software problems, and that will not meet all requirements.

The Air Force is worried about the progress of this acquisition. It will be delivered 8 years late, will cost at least $600 million more than planned, will not have the capabilities originally promised, and will not meet CMU's long-term information needs. The Air Force knows it needs a system that can evolve along with changes in programs and missions. Having a system that can adapt to change is essential for the CMU program not only because missions may be changed or be added, but because technological improvements that could allow the Air Force to perform its mission more quickly and at less cost are inevitable.

The Air Force's current approach is flawed. Until the Air Force performs the analysis needed to define an overall CMU system architecture, it will continue to waste resources and face serious development and integration problems. Since CMU development will continue past 1995, it is not too late for the Air Force to define an architecture to guide the development of this important system to meet current and future missions.

[4]GAO/IMTEC-91-23, Apr. 10, 1991.

## Recommendation to the Secretary of Defense

We recommend that the Secretary of Defense direct the Secretary of the Air Force to perform the analyses needed to define an overall CMU system architecture. This architecture should be derived from the requirements of current and potential future CMU missions, and should be used as a guide to develop a system that can effectively provide attack warning and attack assessment information into the 21st century.

As agreed with your office, we did not request formal comments on a draft of this report from the Department of Defense. However, we discussed the information contained in it with appropriate Defense program officials, including the Vice Commander, Air Force Space Command and the Director of Command and Control Systems, U.S. Space Command. The Director of Command and Control Systems confirmed that CMU is not being developed as an integrated system. He said the subsystems began as individual acquisitions, and they continue to be developed as separate acquisitions.

Nevertheless, these Air Force officials recognized the importance of having a system architecture. The Air Force is working on a study known as NUICCS (NORAD/U.S. Space Command Integrated Command and Control System) to identify and evaluate the various systems which make up the infrastructure supporting NORAD and U.S. Space Command missions, including ITW/AA. The Air Force has realized that standards and criteria for such areas as engineering and configuration management are needed to ensure that the various systems, including CMU, can operate in concert to accomplish NORAD and U.S. Space Command missions. However, the Air Force did not provide any specific evidence on how the NUICCS effort would directly affect CMU development.

We are providing copies of this report to the Secretary of Defense; the Secretary of the Air Force; the Director, Office of Management and Budget; appropriate House and Senate Committees; and other interested parties. We will also make copies available to others upon request.

We performed our work in accordance with generally accepted government auditing standards from April 1991 to April 1992. This work was done under the direction of Samuel W. Bowlin, Director for Defense and Security Information Systems, who can be reached at (202) 512-6240. Other major contributors are listed in appendix III.

Sincerely yours,

Ralph V. Carlone
Assistant Comptroller General

# Contents



**Abbreviations**

| | |
|---|---|
| CCPDS-R | Command Center Processing and Display System Replacement |
| CMU | Cheyenne Mountain Upgrade |
| CSSR | Communications System Segment Replacement |
| GAO | General Accounting Office |
| IMTEC | Information Management and Technology Division |
| ITW/AA | Integrated Tactical Warning and Attack Assessment |
| NORAD | North American Aerospace Defense Command |
| NUICCS | NORAD/U.S. Space Command Integrated Command and Control System |
| OPCC | Offut Processing Communication Integration System |
| SCIS | Survivable communications Integration System |
| SPADOC | Space Defense Operations Center IV |

# Objectives, Scope, and Methodology

The Chairman, Subcommittee on Defense, House Appropriations Committee, requested that we determine whether (1) an overall system architecture was used to guide the Air Force's development of the Cheyenne Mountain Upgrade (CMU) program; (2) CMU will be capable of meeting future missions; and (3) requirements trade-offs will affect system capability. To address these questions, we evaluated whether the Air Force generated and used an overall CMU system architecture, or strategic information system plan, to guide these systems' development; whether requirements trade-offs and program modifications will affect the CMU system capability (performance and effectiveness); whether potential future missions' needs were articulated and considered; and whether the systems, as currently designed, are flexible enough to meet future missions of Cheyenne Mountain.

To address design and development efforts, we reviewed and analyzed several strategic information systems planning methodologies intended to structure the development and design process of information systems. Our assessment of the various methodologies and evaluation of the specific approaches and terminology resulted in a generic framework for analyzing, designing, and developing an information system architecture to meet specific information processing needs. This framework was used as the basis for evaluating the CMU effort. We developed an architectural profile on each of the five CMU subsystems' and the backup facility's hardware, software, security, database management, and communications characteristics. These profiles were used to analyze and compare characteristics within and between the CMU subsystems to determine whether the subsystems are compatible with each other and adaptable to future mission changes.

To supplement the architectural profile and to determine whether the Air Force used a strategic plan to guide the upgrade system development effort, we interviewed Department of Defense and Air Force officials and engineering support contractors and reviewed various planning and architectural documents, system specifications, and system requirements documents. To determine to what extent the CMU program was capable of meeting future missions, we also obtained information on future missions that will impact the CMU program, and compared characteristics of these missions with characteristics of the CMU subsystems.

We performed work at the Air Force Space Command, U.S. Space Command, NORAD, and Air Force Logistics Command's Detachment 25 in Colorado Springs, Colorado; Air Force Systems Command's Electronic

Systems Division in Bedford, Massachusetts; and at Air Force Headquarters, the Joint Chiefs of Staff, and Office of the Secretary of Defense at the Pentagon.

As agreed with the Chairman's office, we did not request formal comments on a draft of this report from the Department of Defense. However, we discussed the information contained in it with appropriate Defense program officials, including the Vice Commander, Air Force Space Command and the Director of Command and Control Systems, U.S. Space Command. The Director of Command and Control Systems confirmed that CMU is not being developed as an integrated system. He said the subsystems began as individual acquisitions, and they continue to be developed as separate acquisitions. Our work was performed between April 1991 and April 1992 in accordance with generally accepted government auditing standards.

# The Subsystems Included in the Cheyenne Mountain Upgrade Program

In the early 1980s, the Air Force began modernizing the computers that provide timely warning and assessment information to our nation's leaders in the event of a missile or bomber attack on the United States. This system—known as the Cheyenne Mountain Upgrade (CMU) program—is to enhance the Air Force's communications, data processing, computer displays, and command and control capabilities at Cheyenne Mountain. Five system upgrades and one back-up system—none fully operational to date—comprise the upgrade program. The five subsystems are the (1) Communications System Segment Replacement (CSSR); (2) Space Defense Operations Center 4 (SPADOC 4); (3) Command Center Processing and Display System Replacement (CCPDS-R); (4) Survivable Communications Integration System (SCIS); and (5) Granite Sentry. The back-up system is the Offutt Processing and Correlation Center (OPCC) at Offutt Air Force Base in Nebraska and it will provide missile warning and air defense information should the system at Cheyenne Mountain fail.

The six subsystems that comprise the CMU, when operational, will work together to form one integrated system. Warning of an attack will be picked up by missile, atmospheric, and space sensors. Missile information will then be passed to the SCIS subsystem, which will send it through various communications media to the CSSR subsystem and national decision makers. The atmospheric and space sensors that detect bomber and space information will pass this information directly to CSSR. CSSR will act as a message switch and route the messages to the mission centers in Cheyenne Mountain—CCPDS-R for missile information, SPADOC 4 for space information, and Granite Sentry for atmospheric and missile information. Granite Sentry displays will also integrate information from the air, space, and missile mission areas. A description of the CMU subsystems follows:

## Communications System Segment Replacement

The CSSR program is intended to ensure uninterrupted communications to, from, and among ITW/AA subsystems. Messages received from the various missile, air, and space sensors are to be distributed by this subsystem to the upgraded mission control centers at Cheyenne Mountain for further processing. Through October 1988, this replacement subsystem was being developed in two separate blocks. Block I is a semiautomated technical control unit that is intended to automate the monitoring and technical control of communications lines entering Cheyenne Mountain. Block II is a message distribution subsystem that receives messages, checks them for completeness, and forwards them to various NORAD computer systems for processing. In November 1988, the Air Force consolidated these blocks into one replacement program.

| | |
|---|---|
| Space Defense Operations Center 4 | The SPADOC 4 program is intended to be a data processing and communications center that can monitor space activities, provide timely warning of any threat or attack, and protect satellites by identifying and suggesting satellite maneuvers to avoid threats. It will automate manual functions and enhance space defense and surveillance. The program is being implemented in three blocks. The first two blocks are currently operational; the final block will complete the automated capability needed to consolidate United States Space Command's space defense data processing functions into one command and control center. |
| Survivable Communications Integration System | The SCIS program is intended to enhance the survivability of NORAD's communications by providing the capability to transmit critical missile warning messages simultaneously over multiple communications media. Originally, it was intended to provide (1) a secure voice capability between individual sensor sites and command centers and (2) a capability to transmit messages over five different communications media. Recently, the number of communications systems was reduced from five to three. |
| Command Center Processing and Display System Replacement | The CCPDS-R program is intended to replace the current missile warning data processing system. Its purpose is to provide standardized ballistic missile warning display systems for national decision makers. |
| Granite Sentry | The Granite Sentry program, once operational, is to improve a variety of attack warning and assessment missions. The program will replace the modular display system and the air defense portion of the NORAD computer system. Granite Sentry will be implemented in several phases to upgrade (1) the Air Defense Operations Center; (2) the NORAD Command Center; (3) air, missile, and space warning displays; (4) interfaces to other Cheyenne Mountain subsystems; and (5) the Battle Staff Support Center and Weather Support Unit. |
| Offutt Processing and Correlation Center | OPCC is a new capability that will be a back-up facility for Cheyenne Mountain. It is intended to operate as an austere version of Cheyenne Mountain and be able to perform critical ITW/AA and command, control, and communications functions until it is physically destroyed. It will consist of a subset of CSSR, SCIS, and CCPDS-R. In addition, it will include Granite Sentry, a terminal for receiving intelligence data from the Strategic Air Command, and a terminal for receiving space information. |

# Major Contributors to This Report

| | |
|---|---|
| Information Management Technology Division, Washington, D.C. | Michael T. Blair, Jr., Assistant Director<br>Leonard J. Latham, Technical Assistant Director<br>Sally M. Obenski, Senior Evaluator |
| Denver Regional Office | Frederick G. Day, Regional Management Representative<br>Sigrid L. McGinty, Evaluator-in-Charge<br>David A. Powner, Site Senior<br>Michael L. Gorin, Evaluator<br>Keith A. Rhodes, Technical Advisor |

# Related GAO Products

Computer Technology: Air Attack Warning System Cannot Process All Radar Track Data (GAO/IMTEC-91-15, May 13, 1991).

Attack Warning: Costs to Modernize NORAD's Computer System Significantly Understated (GAO/IMTEC-91-23, Apr. 10, 1991).

Defense Acquisition: Air Force Prematurely Recommends ADP Acquisitions (GAO/IMTEC-90-07, Mar. 29, 1990).

Attack Warning: Defense Acquisition Board Should Address NORAD's Computer Deficiencies (GAO/IMTEC-89-74, Sept. 13, 1989).

Attack Warning: Better Management Required to Resolve NORAD Integration Deficiencies (GAO/IMTEC-89-26, July 7, 1989).

Space Defense: Management and Technical Problems Delay Operations Center Acquisition (GAO/IMTEC-89-18, Apr. 20, 1989).

Attack Warning: NORAD's Communications System Segment Replacement Program Should Be Reassessed (GAO/IMTEC-89-1, Nov. 30, 1988).